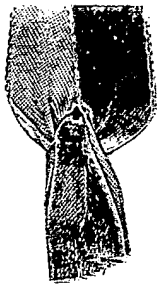


#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

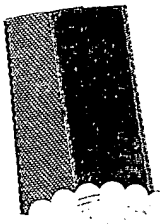
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

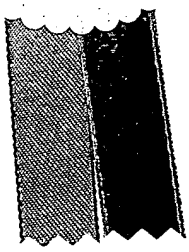
出願年月日
Date of Application: １９９９年１２月 ７日

出願番号
Application Number: 平成１１年特許願第３４７５６２号

出願人
Applicant (s): 株式会社デンソー

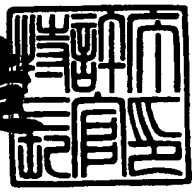


CERTIFIED COPY OF
PRIORITY DOCUMENT



２０００年１１月１７日

特許庁長官
Commissioner,
Patent Office 及川耕造



出証番号 出証特２０００－３０９５８４１

【書類名】　特許願
【整理番号】　PNID3242
【提出日】　平成11年12月 7日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 9/06
【発明者】
【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
【氏名】　菅沼　武史
【発明者】
【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
【氏名】　藤井　義光
【発明者】
【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
【氏名】　穂塚　稔
【特許出願人】
【識別番号】　000004260
【氏名又は名称】　株式会社デンソー
【代理人】
【識別番号】　100082500
【弁理士】
【氏名又は名称】　足立　勉
【電話番号】　052-231-7835
【手数料の表示】
【予納台帳番号】　007102
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【包括委任状番号】　9004766

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　電子制御装置の制御情報書換システム

【特許請求の範囲】

【請求項１】

車両を制御するために車載され、前記制御のための制御情報を電気的に書き換え可能な不揮発性メモリに記憶した電子制御装置と、

前記制御情報を書き換えるための書換装置とを備え、

前記書換装置は、所定のアクセス情報を用いた通信開始処理を前記電子制御装置との間で実行し、

一方、前記電子制御装置は、前記通信開始処理によって前記書換装置の正当性を判断し、当該書換装置が正当であると判断すると、前記書換装置から送信される変更データに基づき前記制御情報の一部又は全部を書き換える制御情報書換システムにおいて、

さらに、前記書換装置との間でデータ通信を行うセンタを備え、

前記センタは、

前記所定のアクセス情報、前記書換装置の識別情報及び当該識別情報に対応する対応情報を記憶した記憶手段と、

前記書換装置とのデータ通信において、当該書換装置の識別情報及び対応情報を取得し、当該取得した情報の対応関係が前記記憶手段に記憶された対応関係と一致している場合は、前記記憶手段に記憶された前記アクセス情報を前記書換装置へ送信し、一方、一致していない場合は、前記アクセス情報を前記書換装置へ送信しない正当性判断手段とを有すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項２】

請求項１に記載の制御情報書換システムにおいて、

前記書換装置は、前記アクセス情報として電子制御装置に記憶された関数Ｆに対応する関数ｆを前記センタから取得し、前記電子制御装置から送信される所定値ｒに対する関数値ｆ（ｒ）を電子制御装置に送信し、

一方、電子制御装置は、前記書換装置から送信される関数値ｆ（ｒ）に対する

関数値Ｆ（ｆ（ｒ））が前記送信した所定値ｒに等しければ、前記書換装置が正当であると判断すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項３】

請求項２に記載の制御情報書換システムにおいて、

前記所定値ｒは、前記電子制御装置にて生成される乱数であること

を特徴とする電子制御装置の制御情報書換システム。

【請求項４】

請求項１～３のいずれかに記載の制御情報書換システムにおいて、

前記電子制御装置は、前記書換装置が正当でないと所定回数判断すると、前記書換装置からのアクセスを一定時間拒否すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項５】

請求項１～４のいずれかに記載の制御情報書換システムにおいて、

前記対応情報は、前記センタとのデータ通信可能状態が確立される毎に、利用者によって前記書換装置へ入力され、

前記書換装置は、前記識別情報と共に前記利用者によって入力された前記対応情報を前記センタへ送信すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項６】

請求項１～４のいずれかに記載の制御情報書換システムにおいて、

前記センタと前記書換装置との間に電話回線を介してデータ通信可能状態が確立されるよう構成されており、

前記センタは、前記データ通信可能状態が確立されると、前記書換装置側の電話番号を前記対応情報として取得すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項７】

請求項１～６のいずれかに記載の制御情報書換システムにおいて、

前記センタは、前記正当性判断手段にて前記対応関係の不一致が所定回数判断

されると、前記書換装置からのアクセスを一定時間拒否すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項８】

請求項１～７のいずれかに記載の制御情報書換システムにおいて、

前記センタは、

さらに、前記制御情報の変更データを記憶する変更データ記憶手段を有しており、

前記電子制御装置にて前記書換装置が正当であると判断された場合に、変更情報記憶手段に記憶された変更データを前記書換装置へ送信すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項９】

請求項８に記載の制御情報書換システムにおいて、

前記電子制御装置は、前記書換装置が正当であると判断すると、前記車両を特定するための車両情報を書換装置へ送信し、

前記センタは、

さらに、前記車両に係る前記制御情報の更新履歴を記憶する更新履歴記憶手段を有しており、

前記電子制御装置からの前記車両情報が前記書換装置によって送信されると、当該車両情報に基づき前記更新履歴記憶手段に記憶された更新履歴を参照し、当該車両において前記制御情報の書き換えの必要性を判断し、書き換えが必要であると判断すると、前記変更データ記憶手段に記憶された変更データを前記書換装置へ送信すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項１０】

請求項１～９のいずれかに記載の制御情報書換システムにおいて、

前記センタは、前記電子制御装置にて前記制御情報の書き換えが完了すると、前記更新履歴記憶手段に記憶された、当該電子制御装置が搭載された車両に対する前記更新履歴を更新すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項１１】

請求項１～１０のいずれかに記載の制御情報書換システムにおいて、

前記書換装置は、前記電子制御装置にて前記制御情報の書き換えが完了すると、前記所定のアクセス情報を抹消すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項１２】

請求項１～１１のいずれかに記載の制御情報書換システムにおいて、

前記書換装置と前記センタとの間でデータ通信可能状態が確立された後、前記電子制御装置にて前記制御情報の書き換えが完了する前に前記書換装置と前記センタとの間のデータ通信が不能となった場合、前記書換装置が前記制御情報の書き換えを中止すること

を特徴とする電子制御装置の制御情報書換システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電気的にデータの書き換えが可能な不揮発性メモリを有する電子制御装置（以下「ＥＣＵ」ともいう。）に関し、特に当該不揮発性メモリに記憶された制御プログラムや制御データといった制御情報の不正な書き換えを防止する技術に関する。

【０００２】

【従来の技術】

従来より、自動車のエンジン等を制御するＥＣＵには、電気的にデータの書き換えが可能な不揮発性メモリに制御情報を格納したものがある。ここで制御情報とは、制御用のプログラム及びデータをいう。これによって、このような制御情報を、市場への供給後でも書き換え可能にしている。

【０００３】

すなわち、この種のＥＣＵは、通常時には、不揮発性メモリに格納された制御情報に従ってエンジン等の制御対象を制御するための制御処理を実行するのであるが、別途用意された書換装置が接続されて、その書換装置から書き換え指令が

送信されて来ると、所定の通信手順を踏んだ後に、不揮発性メモリの内容を書き換えるように構成されている。なお、不揮発性メモリの内容の書き換えは、不揮発性メモリに格納されている制御情報の一部又は全部を消去し、その消去したメモリ領域に、メモリ書換装置から送信されてくる変更データとしての新たな制御情報を書き込むという手順で行われる。

【０００４】

具体的には図９に示すように、車両１００に用意された車両ダイアグコネクタ１２０を介して書換装置２００が接続される。図９では、車両１００に４つのＥＣＵ１０１，１０２，１０３，１０４が搭載されており、各ＥＣＵ１０１～１０４は、ネットワーク回線１１０にて結ばれている。書換装置２００は、作業者による操作に基づきＥＣＵコードを送信することによって、４台のＥＣＵ１０１～１０４のうちの１台とデータ通信を行う。

【０００５】

このようなＥＣＵでは、不揮発性メモリに格納される制御情報を書換装置を用いて書き換えることができるため、動作内容（制御内容）を任意に変更することができるという点で有利である。特に、動作内容（制御内容）に不具合があった場合も迅速に対応できることになり、市場への供給後における車両のメンテナンスを容易にする。

【０００６】

しかしその反面、利用者が制御情報を故意に書き換える可能性が残される。すなわち、環境面や安全面を配慮して設定される制御情報を、利用者が快適性や興味などで書き換えてしまう可能性がある。例えば、エンジンを制御するＥＣＵでは、車速の上限値を制御データとして予め設定しておき、車速がその上限値を越えた場合には、燃料をカットするというような安全面からの制御を行うのが一般的である。このとき、利用者が、予め設定された車速の上限値（制御データ）を故意に書き換えることが考えられる。このように制御情報が利用者によって故意に書き換えられると、環境面や安全面において妥当でない状況が発生する。

【０００７】

そのため、Ｅ－ＯＢＤの電子システムセキュリティ規定で不正な制御情報の書

き換えを防止することが義務付けられている。そこで次に、従来の書換処理を図面を用いて説明する。

図１０の左側に示した処理が図９におけるＥＣＵ１０１～１０４の処理に相当し、図１０の右側に示した処理が図９における書換装置２００の処理に相当している。なお、各処理にはｂ１～ｂ１２の符号を付した。以下、この符号を用いて処理の説明を行う。

【０００８】

まず最初に書換装置が制御情報の書き換えを行うＥＣＵを選択し、書換要求を送信する（ｂ１）。ＥＣＵの選択は、ＥＣＵコードを送信することによって行う。このＥＣＵコードは作業者によって書換装置に入力される。すると、選択されたＥＣＵは、乱数ｒを発生し（ｂ２）、この乱数ｒを書換装置へ送信する（ｂ３）。

【０００９】

書換装置には関数ｆが予め記憶されており、送信される乱数ｒに対して関数値ｆ（ｒ）を算出する（ｂ４）。そして、その算出した関数値ｆ（ｒ）を送信する（ｂ５）。一方、ＥＣＵには関数Ｆが予め記憶されており、送信される関数値ｆ（ｒ）に対して関数値Ｆ（ｆ（ｒ））を算出する（ｂ６）。続いて、算出したＦ（ｆ（ｒ））が乱数ｒに等しければ、すなわち$f = F^{-1}$であれば、書き換えを許可する許可信号を送信する（ｂ７）。

【００１０】

ここまでの処理は、ＥＣＵが記憶する関数Ｆの逆関数ｆを書換装置が有している場合に、ＥＣＵが書換装置を正当であると判断するものである。この例では、書換装置の有する関数ｆがＥＣＵをアクセスするための情報となっている。

書換装置は、ＥＣＵから送信される許可信号を受信すると（ｂ８）、変更データを送信する（ｂ９）。ＥＣＵは、この変更データに基づき制御情報の書き換えを行う（ｂ１０）。

【００１１】

ＥＣＵは制御情報の書き換えが正常に終了すると、正常終了を通知し（ｂ１１）、書換装置が通知を受けて（ｂ１２）一連の書き換え処理が完了する。

【００１２】

【発明が解決しようとする課題】

図１０を用いて説明した書換処理では、書換装置内の情報である関数ｆを用いた通信処理（ｂ１～ｂ７）によって、ＥＣＵが書換装置の正当性を判断している。そのため、書換装置自体が盗まれたり、又は、書換装置内部の情報が盗まれたりした場合には、不正な制御情報の書き換えを防止できないという問題があった。特に、書換装置は作業現場にあるため、上述した盗難の可能性が比較的高くなってしまう。

【００１３】

本発明は、上述した問題点を解決するためになされたものであり、書換装置又は書換装置内部の情報が盗まれた場合であっても、上述した不正な制御情報の書き換えを防止できるようにすることを目的とする。

【００１４】

【課題を解決するための手段及び発明の効果】

上述した目的を達成するためになされた請求項１に記載の制御情報書換システムは、車両を制御するために車載され、制御のための制御情報を電気的に書き換え可能な不揮発性メモリに記憶した電子制御装置と、制御情報を書き換えるための書き換え装置とを備えることを前提としている。

【００１５】

このとき、書換装置は、所定のアクセス情報を用いた通信開始処理を電子制御装置との間で実行し、一方、電子制御装置は、通信開始処理によって書換装置の正当性を判断し、当該書換装置が正当であると判断すると、書換装置から送信される変更データに基づき制御情報の一部又は全部を書き換える。

【００１６】

このような構成に加え、本発明のシステムではさらに、書換装置との間でデータ通信を行うセンタを備えていることを特徴としている。センタは、例えば作業現場とは別の場所に設置されることが考えられる。

このセンタの記憶手段には、上述したアクセス情報が記憶されている。また、書換装置の識別情報及び対応情報が記憶されている。識別情報は、書換装置を識

別するための書換装置固有の番号などであることが考えられる。一方、対応情報は、各識別情報に対応させて設定される情報である。

【００１７】

センタの正当性判断手段は、書換装置とのデータ通信において、当該書換装置の識別情報及び対応情報を取得する。そして、当該取得した情報の対応関係が記憶手段に記憶された対応関係と一致している場合は、所定のアクセス情報を書換装置へ送信する。一方、一致していない場合は、所定のアクセス情報を書換装置へ送信しない。

【００１８】

つまり、本発明では、電子制御装置へのアクセスを可能にするアクセス情報を、書換装置ではなくセンタに記憶しておき、書換装置が正当であることをセンタが判断した場合に、センタからアクセス情報を送信する。

これは、以下のような２段階のチェックを行うことにあたる。

【００１９】

①センタが書換装置の正当性を判断してアクセス情報を書換装置へ送信する。

②書換装置はそのアクセス情報を用いた通信開始処理を実行し、その通信開始処理に基づき、電子制御装置が書換装置の正当性を判断する。

上記①の段階の正当性判断を、識別情報と対応情報との対応関係で行う。

【００２０】

これによって、少なくとも識別情報又は対応情報のいずれか一方を書換装置内部に記憶しておかなければ、上記①の段階で書換装置はセンタからアクセス情報を得ることができない。したがって、書換装置又は書換装置内部の情報が盗まれたとしても、上記②において電子制御装置により書換装置が正当であると判断されないため、その後、制御情報の書き換えが行われない。その結果、書換装置や書換装置内の情報が盗まれた場合であっても、電子制御装置の制御情報が不正に書き換えられることを防止できる。

【００２１】

ところで、上記②における「アクセス情報を用いた通信開始処理」とは、従来技術として既に述べた従来と同様の処理とすることが一例として考えられる。す

なわち、請求項２に示す構成とすることが考えられる。

この場合は、書換装置が、電子制御装置に記憶された関数Ｆに対応する関数ｆをアクセス情報としてセンタから取得し、電子制御装置から送信される所定値ｒに対する関数値ｆ（ｒ）を電子制御装置に送信する。一方、電子制御装置は、書換装置から送信される関数値ｆ（ｒ）に対する関数値Ｆ（ｆ（ｒ））が送信した所定値ｒに等しければ、すなわち、$F = f^{-1}$（$f = F^{-1}$）であれば書換装置が正当であると判断する。なお、所定値ｒは固定的なものとしてもよいが、請求項３に示すように、乱数を用いることが考えられる。

【００２２】

なお、正当なアクセス情報を得ることなく、書換装置による電子制御装置への不正なアクセスが行われることを防止するために、請求項４に示す構成を採用してもよい。この構成では、電子制御装置が、書換装置を正当でないと所定回数判断すると、書換装置からのアクセスを例えば１０分というような一定時間拒否する。所定回数は１回としてもよいが、通信エラーなどが生じる可能性を考慮して例えば３回というように設定することが考えられる。また、所定回数は、「正当でない」という判断が連続して行われた回数であってもよいし、「正当でない」という判断を累積した回数としてもよい。このようにすれば、不正なアクセス情報を用いては連続的に何度も電子制御装置をアクセスすることができないため、不正な電子制御装置へのアクセスを効果的に防止することができ、制御情報の書き換え防止に有効である。

【００２３】

ところで、上記①における書換装置の正当性判断において、センタは、書換装置の識別情報及び対応情報の対応関係を利用している。

したがって、上述したように、識別情報又は対応情報の少なくともいずれか一方を書換装置内部に記憶しておかなければ、書換装置又は書換装置内部の情報が盗まれた場合であっても、書換装置はセンタからアクセス情報を得ることはできない。

【００２４】

そこで、例えば請求項５に示すように、少なくとも対応情報は、センタとのデ

ータ通信可能状態が確立する度に、利用者によって書換装置へ入力されるようにするとよい。このとき、書換装置は、識別情報と共に、利用者によって入力された対応情報をセンタへ送信する。

【００２５】

ここでいう対応情報は、識別情報に対応するいわゆるパスワードとして位置付けられる。このように毎回利用者が対応情報を入力するようにすれば、書換装置又は書換装置内の情報が盗まれ識別情報が盗まれたとしても、それに対応する対応情報が分からないため、センタからアクセス情報を得ることができない。したがって、電子制御装置の制御情報が不正に書き換えられることを防止できる。

【００２６】

なお、「少なくとも対応情報」としたのは、上述したように識別情報も、書換装置内部に記憶しておかず、例えば対応情報と同様に利用者によって入力されるようにしてもよいためである。その場合、利用者が入力する情報は増えるものの、書換装置又は書換装置内部の情報が盗まれた場合に対応情報だけでなく識別情報までも分からないため、センタからアクセス情報を不正に得られる可能性がさらに低くなり、制御情報が不正な書き換えに対して有効となる。

【００２７】

ただし、対応情報をあるいは識別情報と対応情報とを利用者が入力する上述の構成を採用しても、それらの情報が何らか別のルートで盗まれる可能性も考えられる。そこで、請求項６に示す構成を採用することが考えられる。

この構成は、センタと書換装置との間に電話回線を介してデータ通信可能状態が確立されることを前提とする。センタは、書換装置との間にデータ通信可能状態が確立されると、書換装置側の電話番号を対応情報として取得する。このとき、センタは、取得される識別番号と電話番号との対応が記憶手段に予め記憶された対応と一致するか否かを判断し、一致すればアクセス情報を送信する。

【００２８】

このようにすれば、別の場所、すなわち正規の作業場所以外からセンタとの間に回線を接続した場合、センタの取得する対応情報としての電話番号は予め決められた電話番号でなくなる。そのため、識別情報と対応せず、センタからアクセ

ス情報を得ることはできない。つまり、この技術思想は、不正な書き換えが行われる場合には書換装置が正規の設置場所にない、という事実に着目したものである。このようにすれば、書換装置や書換装置内の情報が盗まれた場合であっても、電子制御装置の制御情報が不正に書き換えられることを確実に防止できる。

【００２９】

ところで、電子制御装置にて書換装置が正当でないと判断された場合に、電子制御装置が書換装置からのアクセスを例えば１０分というような一定時間拒否することによって、電子制御装置への不正なアクセスが効果的に防止できることは上述した。センタと書換装置との間にも、同様の手法を採用することが考えられる。

【００３０】

すなわち請求項７に示すように、センタは、正当性判断手段にて対応関係の不一致が所定回数判断された場合、書換装置からのアクセスを一定時間拒否するようにするとよい。ここでいう「所定回数」の意味するところは、既に述べた請求項３に記載の所定回数と同様であるため省略する。このようにすれば、センタへの不正なアクセスを連続して何度も行うことができない。したがって、不正な制御情報の書き換えを防止するのに有効である。

【００３１】

ところで従来は、書換装置の有する記録媒体に制御情報を書き換えるための変更データを記憶していた。本発明においても、変更データを書換装置に記憶する構成としてもよい。しかし、さらにセキュリティ面を考慮するならば、請求項８に示すような構成を採用することが望ましい。

【００３２】

この構成では、センタが、さらに、制御情報の変更データを記憶する変更データ記憶手段を有しており、電子制御装置にて書換装置が正当であると判断された場合に、変更情報記憶手段に記憶された変更データを書換装置へ送信する。

この場合は、書換装置でなくセンタに変更データを記憶しておく。これによって、書換装置又は書換装置内部の情報が盗まれた場合であっても、変更データが外部に漏れる可能性がない。さらに、上記②において書換装置が正当であるとの

判断がなされた後に、変更データを書換装置へ送信する。もちろん、上記①において書換装置の正当性をセンタが判断した場合に、アクセス情報と共に変更データを書換装置へ送信するようにしてもよい。しかし、上述したように電子制御装置にて書換装置が正当であると判断された場合に変更データを送信するようにすれば、すなわち、上記①及び②のチェックが行われた後に変更データを送信するようにすれば、さらにセキュリティ面で有利である。

【００３３】

なお、この場合には、電子制御装置が書換装置を正当なものであると判断すると、書き換えの許可を示す情報を電子制御装置が書換装置へ送信し、さらに、書換装置がこの情報をセンタに送信することによって、センタが変更データを送信するという具合である。

【００３４】

このような構成を前提としてさらなる工夫をすれば、次に示すような問題を解決することができる。

その問題とは、従来、過去に電子制御装置の制御情報が書き換えられているか否かを判断できない状況があったことである。

【００３５】

例えば制御プログラムが複数回バージョンアップされているような場合、ある車両に対して同一ユーザが同一の修理工場を利用する場合は、修理工場側で記録を残すことなどで車両の制御プログラムがどこまでバージョンアップされたかを把握することができる。

【００３６】

しかし、車両のユーザが途中で変わった場合や別の修理工場へ車両の点検を依頼した場合などは、制御プログラムのバージョンアップの履歴がないため、既に制御プログラムの書き換えが行われているにもかかわらず、再度制御プログラムの書き換えを行うというような無駄な制御情報の書き換えが行われる状況があった。このような場合、無駄な作業時間を要するだけでなく、例えば制御情報の記憶にＥＥＰＲＯＭを用いている場合、書き換え可能回数が制限されるため、無駄な書き換えによって必要な書き換えができなくなるおそれもあった。

【００３７】

そこで、請求項９に示すように、請求項８に示した構成に加え、センタが、さらに、車両に係る制御情報の更新履歴を記憶する更新履歴記憶手段を有する構成とすることが考えられる。この場合、電子制御装置は、書換装置が正当であると判断すると、車両を特定するための車両情報を送信する。センタは、電子制御装置からの車両情報が書換装置によって送信されると、当該車両情報に基づき更新履歴記憶手段に記憶された更新履歴を参照する。そして、参照した更新履歴に基づき、当該車両における制御情報の書き換えの必要性を判断し、書き換えが必要であると判断すると、変更データ記憶手段に記憶された変更データを書換装置へ送信する。なお、車両情報は、電子制御装置の搭載された車両を特定するための情報であり、例えば各車両固有の車両ＶＩＮ（Vehicle ID Number ）コードとすることが考えられる。

【００３８】

このようにすれば、センタによって制御情報の更新履歴が管理されるため、無駄な制御情報の書き換えが行われない。その結果、無駄な作業時間がなくなり、また、無駄な書き換えによって必要な書き換えができなくなることもなくなる。

なお、更新履歴は、例えば作業者が制御情報の書き換え完了後にマニュアル操作で更新してもよいが、請求項１０に示すように自動的に更新されるようにすると便利である。

【００３９】

すなわち、センタは、電子制御装置にて前記制御情報の書き換えが完了すると、更新履歴記憶手段に記憶された、当該電子制御装置が搭載された車両に対する更新履歴を更新するようにするとよい。具体的には、電子制御装置が制御情報の書き換えが完了したことを示す情報を書換装置に送信し、書換装置がさらにこの情報をセンタへ送信する。センタは、この情報に基づき、更新履歴を更新するという具合である。このようにすれば、書き換えの終了時に更新履歴が自動的に更新されるため、作業者にとって便利である。

【００４０】

ところで、センタが書換装置の正当性を判断してアクセス情報を送信した後に

、その書込装置からアクセス情報が盗まれる可能性も考えられる。

したがって、請求項１１に示すように、書換装置は、電子制御装置にて制御情報の書き換えが完了すると、所定のアクセス情報を抹消するのが望ましい。具体的には、電子制御装置が制御情報の書き換えが完了したことを示す情報を書換装置へ送信し、この情報に基づき、書換装置がアクセス情報を抹消するという具合である。このようにすれば、書き換えの終了時にアクセス情報が速やかに抹消されるため、一度送信されたアクセス情報が書換装置から盗まれる可能性を低減させることができる。

【００４１】

また、上記①において書換装置がセンタからアクセス情報を取得した後、センタと書換装置との間のデータ通信を一時的に終了することが考えられる。ただし、書換装置に送信されたアクセス情報が盗まれ、別の書換装置を用い、このアクセス情報を使用して電子制御装置がアクセスされる可能性がある。

【００４２】

したがって、請求項１２に示すように、書換装置とセンタとの間でデータ通信可能状態が確立された後、電子制御装置にて制御情報の書き換えが完了する前に書換装置とセンタとの間のデータ通信が不能となった場合、書換装置が制御情報の書き換えを中止するようにすることが考えられる。

【００４３】

この場合、書換装置の正当性判断を含む一連の書き換え処理が終了するまではセンタと書換装置がデータ通信可能状態となっていることを書き換えの条件とするのである。これによって、盗んだアクセス情報を用いて別の書換装置から電子制御装置をアクセスすることができないため、制御情報が不正な書き換えを確実に防止できる。

【００４４】

【発明の実施の形態】

以下、本発明を具体化した一実施例を図面を参照して説明する。

図１は、実施例の制御情報書換システム１の概略構成を示すブロック図である。車両１０には、４台のＥＣＵ１１，１２，１３，１４が搭載されており、各Ｅ

ＣＵ１１～１４はネットワーク回線１５で結ばれている。ＥＣＵ１１～１４は、不揮発性メモリとしてのＥＥＰＲＯＭ（不図示）を有しており、書換装置２０が接続されていない通常時には、このＥＥＰＲＯＭに記憶された制御情報（制御プログラム及び制御データ）に基づき、ネットワーク回線１５を介したＥＣＵ１１～１４間通信を行って、エンジン等それぞれの制御対象を制御する。

【００４５】

そして、ＥＣＵ１１～１４の有するＥＥＰＲＯＭに記憶された制御情報を書き換えるためのシステムが、本制御情報書換システム１である。

図１では、書換装置２０が車両ダイアグコネクタ１６を介して各ＥＣＵ１１～１４と接続された様子が示されている。車両ダイアグコネクタ１６は、書換装置２０と各ＥＣＵ１１～１４とのネットワーク回線１５を介したデータ通信を可能にするため、車両１０に用意されたコネクタである。なお、車両１０及び書換装置２０は、修理工場などの作業現場に設置されている。

【００４６】

また、本実施例の制御情報書換システム１では、書換装置２０が電話回線網４０を介してセンタ３０とデータ通信できるようになっている。センタ３０は、いわゆるサーバとして作業現場とは別の場所に設置される。そして、このセンタ３０の記憶装置（不図示）には、ＥＣＵ１１～１４を書換装置２０がアクセスするためのアクセス情報、制御情報を書き換える変更データ、書換装置２０の正当性を判断するためのデータベース、及び、各車両１０の制御情報の更新履歴のデータベースが記憶されている。したがって、この記憶装置が「記憶手段」、「変更データ記憶手段」及び「更新履歴記憶手段」に相当する。

【００４７】

書換装置２０とセンタ３０とは、書換装置２０がセンタ３０を発呼することによって、書換装置２０とセンタ３０との間で所定の通信処理が行われてデータ通信が可能な状態となる。なお、図１には、センタ３０が１台の書換装置２０と接続されていることを示したが、センタ３０に対しては、例えば別の作業現場の書換装置が並行して接続されることも考えられる。

【００４８】

次に、本制御情報書換システム１の動作の概要を図２に基づき説明する。

図２では、本制御情報書換システム１の動作をＢ１～Ｂ１８の符号を付したブロック単位で示した。詳しくは、各ＥＣＵ１１～１４における処理を、ＥＣＵ側処理として図２中の左側の列に、Ｂ５，Ｂ６，Ｂ９，Ｂ１０，Ｂ１５，Ｂ１６と示した。また、書換装置２０における処理を、書換装置側処理として中央の列に、Ｂ１，Ｂ４，Ｂ７，Ｂ８，Ｂ１１，Ｂ１４，Ｂ１７と示した。さらに、センタ３０における処理を、センタ側処理として右側の列に、Ｂ２，Ｂ３，Ｂ１２，Ｂ１３，Ｂ１８と示した。これらの処理は、Ｂ１→Ｂ２→Ｂ３→・・・→Ｂ１８という順序で実行される。

【００４９】

最初に書換装置２０がセンタ３０を発呼し、書換装置２０とセンタ３０との間にデータ通信可能状態が確立されると、書換装置２０は、通信開始要求と共に書換装置２０自体を識別させるための「識別情報」としてのＩＤ情報をセンタ３０へ送信する（Ｂ１）。これに対し、センタ３０は、書換装置２０からのＩＤ情報を受信すると共に、発呼元の電話番号、すなわち、書換装置２０側の電話番号を取得する（Ｂ２）。この電話番号が「対応情報」に相当する。

【００５０】

センタ３０は、書換装置２０のＩＤ情報と書換装置２０に割り当てられた電話番号とを対応させたデータベースを有している。したがって、センタ３０は次に、受信したＩＤ情報と取得した電話番号との対応関係をデータベースにある対応関係と照合する（Ｂ２）。ここで一致していれば、第１許可信号及び関数ｆを書換装置２０へ送信する（Ｂ３）。

【００５１】

書換装置２０は、ＥＣＵ１１～１４の中から書き換え対象とするＥＣＵを選択し、そのＥＣＵへ書換要求を送信する（Ｂ４）。ここではＥＣＵ１１が書き換え対象のＥＣＵとして選択されたものとして以下の説明を続ける。

選択されたＥＣＵ１１は、乱数ｒを発生し（Ｂ５）、この乱数ｒを書換装置２０へ送信する（Ｂ６）。

【００５２】

書換装置２０は、上記Ｂ３にてセンタから送信された関数ｆを用い、ＥＣＵ１１からの乱数ｒに対して関数値ｆ（ｒ）を算出する（Ｂ７）。そして、その算出した関数値ｆ（ｒ）をＥＣＵ１１へ再度送信する（Ｂ８）。

一方、ＥＣＵ１１には関数Ｆが予め記憶されており、書換装置２０から送信される関数値ｆ（ｒ）に対し、関数値Ｆ（ｆ（ｒ））を算出する（Ｂ９）。続いて、算出したＦ（ｆ（ｒ））が乱数ｒに等しければ、すなわち$f=F^{-1}$であれば、書き換えを許可する第２許可信号を送信すると共に、車両ＶＩＮコードを送信する（Ｂ１０）。車両ＶＩＮコードは、車両毎にユニークに付された番号であり、これが上述の「車両情報」に相当する。

【００５３】

書換装置２０は、ＥＣＵ１１からの第２許可信号及び車両ＶＩＮコードを受信し、これらの情報をさらに、センタ３０へ送信する（Ｂ１１）。

センタ３０は、各車両それぞれの制御情報の更新履歴をデータベースとして有している。したがって、書換装置２０からの車両ＶＩＮコードに基づき、車両１０の判別を行い、更新履歴のデータベースを参照して、制御情報の書き換え必要性を判断する（Ｂ１２）。ここで車両１０に対する制御情報の書き換えが必要であると判断すると、変更データを書換装置２０へ送信する（Ｂ１３）。

【００５４】

書換装置２０は、センタ３０からの変更データを受信し、この変更データをＥＣＵ１１へ送信する（Ｂ１４）。

ＥＣＵ１１は、書換装置２０からの変更データに基づき、制御情報の書き換えを行う（Ｂ１５）。そして、制御情報の書き換えが正常に終了すれば、正常終了を書換装置２０へ通知する（Ｂ１６）。

【００５５】

書換装置２０は、ＥＣＵ１１から正常終了が通知されると、上記Ｂ３にてセンタ３０から送信された関数ｆを抹消する（Ｂ１７）。また、センタ３０に正常終了を通知する。これによって、センタ３０は、更新履歴のデータベースを更新する（Ｂ１８）。

【００５６】

以上のようにして一連の書き換え処理が完了する。

次に、上述したＥＣＵ側処理、書換装置側処理、及びセンタ側処理の詳細を順に説明する。なお、各処理の説明にあたって適宜図２を参照する。

最初に図３及び図４のフローチャートに基づき、各ＥＣＵ１１～１４にて実行されるＥＣＵ側処理を説明する。なお、このＥＣＵ側処理は、車両１０に車両ダイアグコネクタ１６を介して書換装置２０が接続された状態において、例えば０．２秒というような所定時間間隔で実行されるものである。

【００５７】

まずステップＳ３００において、書換装置２０からの書換要求があったか否かを判断する。ここで書換要求があったと判断された場合（Ｓ３００：ＹＥＳ）、Ｓ３１０へ移行する。一方、書換要求がなかったと判断された場合（Ｓ３００：ＮＯ）、以降の処理を実行せずに、本ＥＣＵ側処理を終了する。

【００５８】

Ｓ３１０では、アクセス拒否タイマが「０」か否かを判断する。アクセス拒否タイマは、後述するように書換装置２０が「正当でない」と所定回数連続して判断された場合に設定されるものである。ここでアクセス拒否タイマが「０」でないと判断された場合（Ｓ３１０：ＮＯ）、Ｓ３２０にてタイマをデクリメントし、さらに変数Ｃ１に「０」を代入して、本ＥＣＵ側処理を終了する。変数Ｃ１は、書換装置が正当でないと連続して判断された回数を計数するものである。一方、アクセス拒否タイマが「０」であると判断された場合（Ｓ３１０：ＹＥＳ）、Ｓ３３０へ移行する。

【００５９】

Ｓ３３０では、変数Ｃ１が「２」以下であるか否かを判断する。ここでＣ１＞２である場合（Ｓ３３０：ＮＯ）、Ｓ３４０にてアクセス拒否タイマをセットし、本ＥＣＵ側処理を終了する。本実施例では、１０分がセットされる。一方、Ｃ１≦２である場合（Ｓ３３０：ＹＥＳ）、Ｓ３５０へ移行する。

【００６０】

Ｓ３５０では、乱数ｒを発生し、書換装置２０へ送信する。この処理は、図２中のＢ５及びＢ６の処理に相当する。これに対し、図２中のＢ８に示したように

、書換装置２０から関数値ｆ（ｒ）が送信される。

したがって、続くＳ３６０では、関数値ｆ（ｒ）の送信があったか否かを判断する。ここで関数値ｆ（ｒ）の送信があった場合（Ｓ３６０：ＹＥＳ）、Ｓ３７０へ移行する。一方、関数値ｆ（ｒ）の送信がないうちは（Ｓ３６０：ＮＯ）、この判断処理を繰り返す。

【００６１】

Ｓ３７０では、書換装置２０から送信される関数値ｆ（ｒ）に対し、関数値Ｆ（ｆ（ｒ））を算出する。この処理は、図２中のＢ９の処理に相当する。

続く図４のＳ３８０では、算出した関数値Ｆ（ｆ（ｒ））が乱数ｒに等しいか否かを判断する。ここでＦ（ｆ（ｒ））＝ｒである場合（Ｓ３８０：ＹＥＳ）、Ｓ３９０にて第２許可信号及び車両ＶＩＮコードを送信し、Ｓ４２０へ移行する。このＳ３８０及びＳ３９０の処理が図２中のＢ１０の処理に相当する。一方、Ｆ（ｆ（ｒ））≠ｒである場合（Ｓ３８０：ＮＯ）、書き換えを許可しない旨をＳ４００にて書換装置２０に通知し、Ｓ４１０にて変数Ｃ１をインクリメントして、本ＥＣＵ側処理を終了する。このようにして書換装置２０の正当性が判断され、正当でないと判断した場合（Ｓ３８０：ＮＯ）変数Ｃ１がインクリメントされ（Ｓ４１０）、上述したようにＣ１＞２でタイマがセットされる（図３中のＳ３４０）。したがって、本実施例では、Ｃ１が「０」→「１」→「２」という具合に、３回連続して書換装置２０が正当でないと判断されると、アクセス拒否がなされることになる。

【００６２】

上述したように、センタ３０にて車両ＶＩＮコードに基づく制御情報の書き換えの必要性判断がなされ、書き換えが必要があればセンタ３０から書換装置２０を経由して変更データが送信される。一方、書き換えが必要でなければ、すなわち、既に制御情報の書き換えがなされている場合には、書き換え済みであることを示す情報がセンタ３０から書換装置３０を経由して送信される。

【００６３】

そのため、Ｓ４２０では、書換装置２０からのデータ送信があったか否かを判断する。ここでデータ送信があったと判断された場合（Ｓ４２０：ＹＥＳ）、Ｓ

４３０へ移行する。一方、データ送信がないうちは（Ｓ４２０：ＮＯ）、この判断処理を繰り返す。

【００６４】

そして、Ｓ４３０では、書換装置２０から送信されたデータが変更データか否かを判断する。ここで変更データであると判断された場合（Ｓ４３０：ＹＥＳ）、Ｓ４４０へ移行する。一方、変更データでないと判断された場合（Ｓ４３０：ＮＯ）、すなわち、書き換え済みを示す情報が送信された場合には、以降の処理を実行せず、本ＥＣＵ側処理を終了する。

【００６５】

Ｓ４４０では、送信された変更データに基づき、制御情報の書き換えを行う。続くＳ４５０では、書き換え後の制御情報のチェックサムを計算する。これは、正常に制御情報が書き換えられたか否かを判断するためである。

そして、次のＳ４６０では、Ｓ４５０にて計算したチェックサムに基づき、制御情報の書き換えが正常に終了したか否かを判断する。ここで正常に終了したと判断された場合（Ｓ４６０：ＹＥＳ）、Ｓ４７０にて書換装置２０へ正常終了を通知し、その後、本ＥＣＵ処理を終了する。一方、正常に終了したと判断されなかった場合（Ｓ４６０：ＮＯ）、Ｓ４８０にて書換装置２０へ変更データの再送信を要求し、Ｓ４２０からの処理を繰り返す。

【００６６】

続いて図５及び図６のフローチャートに基づき、書換装置２０にて実行される書換装置側処理を説明する。なお、この書換装置側処理は、書換装置２０とセンタ３０との間にデータ通信可能状態が確立された後、作業者による所定の操作をトリガとして実行されるものである。

【００６７】

まず最初のステップＳ５００において、センタ３０に対し、通信開始を要求すると共に予め記憶されているＩＤ情報を送信する。この処理は、図２中のＢ１の処理に相当する。

センタ３０は、書換装置２０が正当なものであると判断すると、第１許可信号及び関数ｆを送信してくる。

【００６８】

したがって、続くＳ５１０では、センタ３０からの応答があったか否かを判断する。ここでセンタ３０からの応答があったと判断された場合（Ｓ５１０：ＹＥＳ）、Ｓ５２０へ移行する。一方、センタ３０からの応答がないうちは（Ｓ５１０：ＮＯ）、この判断処理を繰り返す。

【００６９】

Ｓ５２０では、センタ３０の応答が不許可の通知か否かを判断する。ここで不許可の通知であると判断された場合（Ｓ５２０：ＹＥＳ）、センタ３０へのアクセスに失敗した旨をＳ５３０にてディスプレイなどの表示装置に表示し、その後、Ｓ５００からの処理を繰り返す。一方、不許可の通知でない場合（Ｓ５２０：ＮＯ）、すなわち第１許可信号及び関数ｆが送信されてきた場合には、Ｓ５４０へ移行する。

【００７０】

Ｓ５４０では、車両１０に搭載された４台のＥＣＵ１１～１４のいずれかを選択するためのＥＣＵコードの入力を作業者に要求する。続くＳ５５０では、ＥＣＵコードの入力があったか否かを判断する。ここでＥＣＵコードの入力があったと判断された場合（Ｓ５５０：ＹＥＳ）、Ｓ５６０へ移行する。一方、ＥＣＵコードの入力がないうちは（Ｓ５５０：ＮＯ）、Ｓ５４０からの処理を繰り返す。なお、ＥＣＵ１１のＥＣＵコードが入力されたものとして以下の説明を続ける。

【００７１】

Ｓ５６０では、書換要求及びＥＣＵコードを送信する。この処理は、図２中のＢ４の処理に相当する。これによって、入力されたＥＣＵコードに対応するＥＣＵ１１が乱数ｒを発生し、その乱数ｒを送信してくる（図３中のＳ３５０）。

したがって、続くＳ５７０では、乱数ｒが送信されたか否かを判断する。ここで乱数ｒが送信されたと判断された場合（Ｓ５７０：ＹＥＳ）、Ｓ５８０へ移行する。一方、乱数ｒが送信されないうちは（Ｓ５７０：ＮＯ）、この判断処理を繰り返す。

【００７２】

Ｓ５８０では、Ｓ５１０にてセンタ３０から送信された関数ｆを用い、乱数ｒ

に対する関数値ｆ（ｒ）を算出する。そして次のＳ５９０にて、関数値ｆ（ｒ）をＥＣＵ１１へ送信する。図２中のＢ７及びＢ８の処理に相当する。

これに対して、ＥＣＵ１１では、図３中のＳ３６０にて肯定判断され、関数値Ｆ（ｆ（ｒ））が算出される（Ｓ３７０）。そして、Ｓ３８０の判断に基づき、第２許可信号の送信又は書き換えを許可しない旨の通知を行う（Ｓ３９０，Ｓ４００）。

【００７３】

したがって、続く図６中のＳ６００では、ＥＣＵ１１の応答があったか否かを判断する。ここでＥＣＵ１１の応答があったと判断された場合（Ｓ６００：ＹＥＳ）、Ｓ６１０へ移行する。一方、ＥＣＵ１１からの応答がないうちは（Ｓ６００：ＮＯ）、この判断処理を繰り返す。

【００７４】

Ｓ６１０では、ＥＣＵ１１から第２許可信号が送信されたか否かを判断する。ここで第２許可信号が送信されたと判断された場合（Ｓ６１０：ＹＥＳ）、Ｓ６２０にて第２許可信号及びその第２許可信号と共に送信される車両ＶＩＮコードをセンタ３０へ送信し、その後、Ｓ６４０へ移行する。この処理が図２中のＢ１１の処理に相当する。一方、第２許可信号が送信されなかった場合（Ｓ６１０：ＮＯ）、すなわち、ＥＣＵ１１から書き換えを許可しない旨が通知された場合には、Ｓ６３０にてセンタ３０に対し不許可となった旨を通知し、その後、図５中のＳ５３０へ移行する。

【００７５】

Ｓ６２０にてセンタ３０に対し第２許可信号及び車両ＶＩＮコードを送信すると、上述したようにセンタ３０は、書き換えの必要性を判断して、書き換えの必要があれば変更データを送信し、一方、書き換えの必要がなければ書き換え済みを示す情報を送信する。

【００７６】

したがって、Ｓ６４０では、センタ３０の応答があったか否かを判断する。ここでセンタ３０の応答があったと判断された場合（Ｓ６４０：ＹＥＳ）、Ｓ６５０へ移行する。一方、センタ３０の応答がないうちは（Ｓ６４０：ＮＯ）、この

判断処理を繰り返す。

【００７７】

Ｓ６５０では、センタ３０から送信されたデータが変更データであるか否かを判断する。ここで変更データであった場合（Ｓ６５０：ＹＥＳ）、Ｓ６８０へ移行する。一方、変更データでない場合（Ｓ６５０：ＮＯ）、すなわち書き換え済みを示す情報がセンタ３０から送信された場合には、関数ｆを抹消して書き換えの必要がない旨を表示し（Ｓ６６０）、書き換え済みを示す情報をＥＣＵ１１へ送信して（Ｓ６７０）、その後、本書換装置側処理を終了する。

【００７８】

Ｓ６８０では、センタ３０から送信された変更データをＥＣＵ１１へ送信する。この処理は、図２中のＢ１４の処理に相当する。これによって、ＥＣＵ１１では制御情報の書き換えが行われ（図４中のＳ４３０：ＹＥＳ，Ｓ４４０）、ＥＣＵ１１から正常終了の通知又は再送信要求がなされる（Ｓ４７０，４８０）。

【００７９】

そこで、次のＳ６９０では、ＥＣＵ１１から正常終了の通知があったか否かを判断する。ここで正常終了の通知があったと判断された場合（Ｓ６９０：ＹＥＳ）、関数ｆを抹消すると共にセンタ３０へ正常終了を通知して（Ｓ７００）、その後、本書換装置側処理を終了する。一方、正常終了の通知がなされない場合（Ｓ６９０：ＮＯ）、すなわち変更データの再送信要求がなされた場合には、センタ３０へ異常終了を通知し（Ｓ７１０）、本書換装置側処理を終了する。

【００８０】

さらに続けて、図７及び図８のフローチャートに基づき、センタ３０にて実行されるセンタ側処理を説明する。なお、このセンタ側処理は、書換装置２０とセンタ３０との間にデータ通信可能状態が確立されている状態において、例えば０．２秒というような所定時間間隔で実行されるものである。

【００８１】

まず最初のステップＳ８００において、アクセス拒否タイマが「０」か否かを判断する。アクセス拒否タイマは、後述するようにセンタ３０によって書換装置２０が「正当でない」と所定回数連続して判断された場合に設定されるものであ

る。ここでアクセス拒否タイマが「０」でないと判断された場合（Ｓ８００：ＮＯ）、Ｓ８１０にてタイマをデクリメントし、さらに変数Ｃ２に「０」を代入して、本センタ側処理を終了する。変数Ｃ２は、センタ３０にて書換装置２０が正当でないと連続して判断された回数を計数するものである。一方、アクセス拒否タイマが「０」であると判断された場合（Ｓ８００：ＹＥＳ）、Ｓ８２０へ移行する。

【００８２】

Ｓ８２０では、変数Ｃ２が「２」以下であるか否かを判断する。ここでＣ２＞２である場合（Ｓ８２０：ＮＯ）、Ｓ８３０にてアクセス拒否タイマをセットし、その後、本センタ側処理を終了する。一方、Ｃ２≦２である場合（Ｓ８２０：ＹＥＳ）、Ｓ８４０へ移行する。

【００８３】

Ｓ８４０では、通信開始要求があったか否かを判断する。この処理は、図５中のＳ５００の処理に対するものである。ここで通信開始要求があったと判断された場合（Ｓ８４０：ＹＥＳ）、Ｓ８５０へ移行する。一方、通信開始要求がないうちは（Ｓ８４０：ＮＯ）、この判断処理を繰り返す。

【００８４】

Ｓ８５０では、書換装置２０から送信されるＩＤ情報を受信し、発呼元の電話番号を取得する。続くＳ８６０では、受信したＩＤ情報と取得した電話番号との対応関係を、データベースに予め記憶された書換装置２０のＩＤ情報と電話番号との対応関係と照合する。これらＳ８５０及びＳ８６０の処理が、図２中のＢ２に示した処理に相当する。

【００８５】

そして、次のＳ８７０では、照合結果に基づき、対応関係が一致したか否かを判断する。ここで一致したと判断された場合（Ｓ８７０：ＹＥＳ）、Ｓ８９０にて第１許可信号及び関数ｆを送信し、その後、Ｓ９００へ移行する。この処理が、図２中のＢ３の処理に相当する。一方、一致していないと判断された場合（Ｓ８７０：ＮＯ）、書き換えを許可しない旨を書換装置２０へ通知すると共に、変数Ｃ２をインクリメントし（Ｓ８８０）、その後、Ｓ８００からの処理を繰り返

す。

【００８６】

なお、ここで説明したＳ８５０～Ｓ８９０までの処理が「正当性判断手段」としての処理に相当する。したがって、これらの処理を実行するセンタ３０のＣＰＵが「正当性判断手段」に相当する。

第１許可信号及び関数ｆを送信した場合、書換装置２０は、第２許可信号及び車両ＶＩＮコードを送信してくるか（図６中のＳ６２０）、あるいは書き換えの不許可を通知してくる（Ｓ６３０）。

【００８７】

そこで、Ｓ９００では、書換装置２０の応答があったか否かを判断する。ここで書換装置２０の応答があったと判断された場合（Ｓ９００：ＹＥＳ）、図８中のＳ９１０へ移行する。一方、書換装置２０の応答がないうちは（Ｓ９００：ＮＯ）、この判断処理を繰り返す。

【００８８】

Ｓ９１０では、その応答が不許可の通知か否かを判断する。ここで不許可の通知であった場合（Ｓ９１０：ＹＥＳ）、図７中のＳ８００へ移行する。一方、不許可の通知でない場合（Ｓ９１０：ＮＯ）、すなわち第２許可信号及び車両ＶＩＮコードが送信された場合には、Ｓ９２０へ移行する。

【００８９】

Ｓ９２０では、送信された車両ＶＩＮコードに基づき車両の判別を行い、更新履歴のデータベースを参照する。そして、次のＳ９３０では、参照結果に基づき、制御情報を書き換える必要があるか否かを判断する。これらＳ９２０及びＳ９３０の処理が図２中のＢ１２の処理に相当する。ここで書き換えの必要があると判断された場合（Ｓ９３０：ＹＥＳ）、Ｓ９５０へ移行する。一方、書き換えの必要がないと判断された場合（Ｓ９３０：ＮＯ）、Ｓ９４０にて書き換え済みを示す情報を送信し、その後、本センタ側処理を終了する。

【００９０】

Ｓ９５０では、変更データを検索して読み出し、読み出した変更データを書換装置２０へ送信する。この処理が、図２中のＢ１３の処理に相当する。その後、

書換装置２０からは、上述したように正常終了の通知（図６中のＳ７００）あるいは異常終了の通知（Ｓ７１０）がなされる。

【００９１】

したがって、Ｓ９６０では、書換装置２０からの終了通知があったか否かを判断する。ここで終了通知があったと判断された場合（Ｓ９６０：ＹＥＳ）、Ｓ９７０へ移行する。一方、終了通知がないうちは（Ｓ９６０：ＮＯ）、この判断処理を繰り返す。

【００９２】

Ｓ９７０では、終了通知が正常終了の通知か否かを判断する。ここで正常終了の通知であると判断された場合（Ｓ９７０：ＹＥＳ）、Ｓ９８０にて更新履歴のデータベースを更新し、その後、本センタ側処理を終了する。一方、正常終了の通知でないと判断された場合（Ｓ９７０：ＮＯ）、すなわち異常終了の通知であった場合には、Ｓ９５０からの処理を繰り返す。

【００９３】

次に、本実施例の制御情報書換システム１の発揮する効果を説明する。なお、ここでの説明に対する理解を容易にするため、最初に従来の問題点を簡単に説明する。

従来は図９に示したように、書換装置２００の正当性を、ＥＣＵ１０１～１０４のみで判断していた。そして、この判断は、書換装置２００に予め記憶されたアクセス情報としての関数ｆに基づく通信開始処理（図１０中のｂ１～ｂ７）によって行われる。そのため、書換装置２００又は書換装置２００内部の情報が盗まれた場合、アクセス情報が盗まれるため、不正な制御情報の書き換えを防止することができなかった。

【００９４】

これに対して、本実施例の制御情報書換システム１では、センタ３０にアクセス情報としての関数ｆを記憶しておき、センタ３０が書換装置２０を正当なものとして判断してはじめて、センタ３０から書換装置２０へ関数ｆが送信される（図２中のＢ２，Ｂ３）。したがって、書換装置２０又は書換装置２０内部の情報が盗まれた場合であっても、書換装置２０にはＥＣＵ１１～１４へのアクセス情

報が記憶されていないため、センタ３０からアクセス情報を得ることができなければ、ＥＣＵ１１～１４の制御情報を書き換えることはできない。

【００９５】

また、センタ３０は、書換装置２０にユニークに割り振られたＩＤ情報と電話回線を介してデータ通信を行う際の書換装置２０側の電話番号とを対応させて記憶したデータベースを有している。そして、書換装置２０からＩＤ情報を取得すると共に発呼元の電話番号を取得する（図７中のＳ８５０）。このＩＤと電話番号との対応関係がデータベースに記憶された対応関係と一致している場合に（Ｓ８６０，Ｓ８７０：ＹＥＳ）、センタ３０は書換装置２０が正当なものであると判断し、アクセス情報である関数ｆを送信する（Ｓ８９０）。例えば正規の作業場所以外からセンタ３０との間に回線を接続した場合、センタ３０の取得する電話番号は予め決められた電話番号でなくなる。そのため、ＩＤ情報と対応せず、センタ３０からアクセス情報を得ることはできない。結果として、ＥＣＵ１１～１４の制御情報を書き換えることはできない。

【００９６】

以上のように、本実施例の制御情報書換システム１によれば、書換装置２０又は書換装置２０内部の情報が盗まれた場合であっても、ＥＣＵ１１～１４の制御情報が不正に書き換えられることを確実に防止できる。

そして、本実施例の制御情報書換システム１では、センタ３０が最初に書換装置２０の正当性を判断し、続いてＥＣＵ１１～１４が書換装置２０の正当性を判断する。これら２段階のチェックのいずれにおいても、書換装置２０が「正当でない」と連続して３回判断された場合、１０分間のアクセス拒否を行うようにした。

【００９７】

すなわち、ＥＣＵ１１～１４では、書換装置２０を正当でないと判断すると（図４中のＳ３８０：ＮＯ）変数Ｃ１をインクリメントし（Ｓ４１０）、変数Ｃ１が「２」よりも大きくなると（図３中のＳ３３０：ＮＯ）、すなわち３回連続して「正当でない」との判断がなされると、アクセス拒否タイマを設定する（Ｓ３４０）。これによって、タイマが「０」となるまで書込装置２０のアクセスを拒

否する（Ｓ３１０：ＮＯ）。

【００９８】

一方、センタ３０でも同様に、書換装置２０を正当でないと判断すると（図７中のＳ８７０：ＮＯ）、変数Ｃ２をインクリメントしていき（Ｓ８８０）、変数Ｃ２が「2」よりも大きくなると（Ｓ８２０：ＮＯ）、すなわち３回連続して「正当でない」との判断がなされると、アクセス拒否タイマを設定する（Ｓ８３０）。これによって、タイマが「０」となるまで書込装置２０のアクセスを拒否する（Ｓ８００：ＮＯ）。

【００９９】

その結果、不正な情報を用いてセンタ３０やＥＣＵ１１～１４を書換装置２０からアクセスしようとしても、連続して何度もアクセスすることができないため、本実施例では３回続けて不正なアクセスを行えば１０分間アクセスができなくなるため、制御情報の書き換え防止に有効である。

【０１００】

また、本実施例の制御情報書換システム１では、センタ３０が制御情報の変更データを記憶している。すなわち、従来のように書換装置２０に変更データを記憶しておかないため、書換装置２０又は書換装置２０内部の情報が盗まれた場合であっても、変更データが外部に漏れる可能性がない。

【０１０１】

そして、センタ３０は、ＥＣＵ１１～１４からの第２許可信号が送信されてきたことを一つの条件として（Ｓ９１０：ＮＯ）変更データを送信する（Ｓ９５０）。すなわち、ＥＣＵ１１～１４にて書換装置２０が正当であると判断されたことを条件として変更データを送信する。したがって、変更データが外部に漏れる可能性をさらに低減させている。

【０１０２】

さらに、ＥＣＵ１１～１４は、書換装置２０を正当であると判断すると（図４中のＳ３８０：ＹＥＳ）、上述した第２許可信号に加え、車両１０を特定可能な車両ＶＩＮコードを送信する（Ｓ３９０）。センタ３０は、各車両１０のＥＣＵ１１～１４に記憶された制御情報更新履歴のデータベースを有しており、上述し

たＥＣＵ１１～１４からの車両ＶＩＮコードに基づき、車両１０を判別しこのデータベースを参照して（図８中のＳ９２０）制御情報の書き換えの必要性を判断する（Ｓ９３０）。そして、書き換えの必要がある場合に（Ｓ９３０：ＹＥＳ）変更データを送信する（Ｓ９５０）。

【０１０３】

従来は、過去にＥＣＵ１１～１４の制御情報が書き換えられているか否かを判断できない状況があった。そのため、制御情報のバージョンアップの履歴がない場合には、既に制御情報の書き換えが行われているにもかかわらず、再度制御情報の書き換えを行うというような無駄な制御情報の書き換えが行われていた。このような場合、無駄な作業時間を要するだけでなく、例えば制御情報の記憶にＥＥＰＲＯＭを用いている場合、書き換え可能回数が制限されるため、無駄な書き換えによって必要な書き換えができなくなるおそれもあった。

【０１０４】

これに対して、本実施例では、上述したようにセンタ３０が各車両１０の制御情報の更新履歴を管理するため、無駄な制御情報の書き換えが行われない。その結果、無駄な作業時間がなくなり、また、無駄な書き換えによって必要な書き換えができなくなることもなくなる。

【０１０５】

さらにまた、本実施例の制御情報書換システム１のセンタ３０では、ＥＣＵ１１～１４から書換装置２０を経由して書き換えの正常終了が通知されると（図８中のＳ９７０：ＹＥＳ）、自動的に制御情報の更新履歴のデータベースを更新する（Ｓ９８０）。したがって、作業者がマニュアル操作でデータベースを更新する必要がなく便利である。

【０１０６】

また、本実施例の制御情報書換システム１の書換装置２０では、アクセス情報としての関数ｆが必要なくなると（図６中のＳ６５０：ＮＯ，Ｓ６９０：ＹＥＳ）、速やかにそのアクセス情報である関数ｆを抹消する（Ｓ６６０，Ｓ７００）。そのため、センタ３０から書換装置２０へ送信されたアクセス情報としての関数ｆが書換装置２０から盗まれる可能性を低減させることができる。

【０１０７】

以上、本発明はこのような実施例に何等限定されるものではなく、本発明の主旨を逸脱しない範囲において種々なる形態で実施し得る。

（１）上記実施例においては、センタ３０が書換装置２０から発呼され、その後、センタ３０と書換装置２０との間にデータ通信可能状態が確立されると、センタ３０は、対応情報として発呼元の電話番号を取得し、書換装置２０から送信される識別情報としてのＩＤ情報との対応によって、書換装置２０の正当性を判断していた。

【０１０８】

これに対して、センタ３０が書換装置２０のＩＤ情報とパスワードとを対応させたデータベースを有する構成とし、書換装置２０は、作業者によって入力されるパスワードを、上述したＩＤ情報と共に送信する構成としてもよい。この場合、パスワードが「対応情報」に相当することになり、センタ３０は、書換装置２０から送信されるＩＤ情報とパスワードとの対応によって、書換装置２０の正当性を判断する。

【０１０９】

また、上記実施例では、書換装置２０に予めＩＤ情報が記憶されていたが、ＩＤ情報も、パスワードと同様に利用者から入力されるようにしてもよい。

このようにすれば、書換装置２０又は書換装置２０内部の情報が盗まれた場合であっても、パスワード、あるいは、ＩＤ情報及びパスワードが分からないため、センタ３０からアクセス情報を得ることはできず、上記実施例と同様に制御情報の不正な書き換えを防止することができる。

【０１１０】

ただし、ＩＤ情報やパスワードが何らか別のルートで盗まれる可能性もあるため、上記実施例のように書換装置２０の設置場所に関連する電話番号を対応情報とすることがより好ましい。不正な書き換えは正規の作業現場では行われないためである。

【０１１１】

（２）また、書換装置２０がセンタ３０からアクセス情報を取得した後、セン

タ３０と書換装置２０との間のデータ通信を一時的に終了することが考えられる。例えば、図２中のＢ１～Ｂ４の通信処理が終了した後に一旦データ通信を終了し、Ｂ１１以降の処理を行う際に、書換装置２０とセンタ３０との間にデータ通信可能状態を再度確立することが考えられる。

【０１１２】

ただし、書換装置２０に送信されたアクセス情報が盗まれ、別の書換装置を用い、このアクセス情報を使用してＥＣＵ１１～１４がアクセスされる可能性がある。

したがって、一連の書き換え処理（図２に示すＢ１～Ｂ１８の処理）が終了するまで、センタ３０と書換装置２０がデータ通信可能状態となっていることを書き換えの条件とするとよい。

【０１１３】

具体的には次のように構成することが考えられる。それは、書換装置２０がタイマ割込処理などによって定期的にセンタ３０へ応答要求を送信し、センタ３０が応答を行う構成とする。このとき、一連の書き換え処理が完了する前にセンタ３０からの応答がなくなった場合、書換装置２０がＥＣＵ１１～１４の書き換えを行わないようにする。このようにすれば、盗んだアクセス情報を用いて別の書換装置からＥＣＵをアクセスすることができなくなる。

【図面の簡単な説明】

【図１】実施例の制御情報書換システムの構成を示すブロック図である。

【図２】実施例における書き換え処理の概要を示す説明図である。

【図３】ＥＣＵ側処理の前半部分を示すフローチャートである。

【図４】ＥＣＵ側処理の後半部分を示すフローチャートである。

【図５】書換装置側処理の前半部分を示すフローチャートである。

【図６】書換装置側処理の後半部分を示すフローチャートである。

【図７】センタ側処理の前半部分を示すフローチャートである。

【図８】センタ側処理の後半部分を示すフローチャートである。

【図９】従来の制御情報書換システムの構成を示すブロック図である。

【図10】従来の書き換え処理の概要を示す説明図である。

【符号の説明】

１…制御情報書換システム

１１，１２，１３，１４…ＥＣＵ

１５…ネットワーク回線

１６…車両ダイアグコネクタ

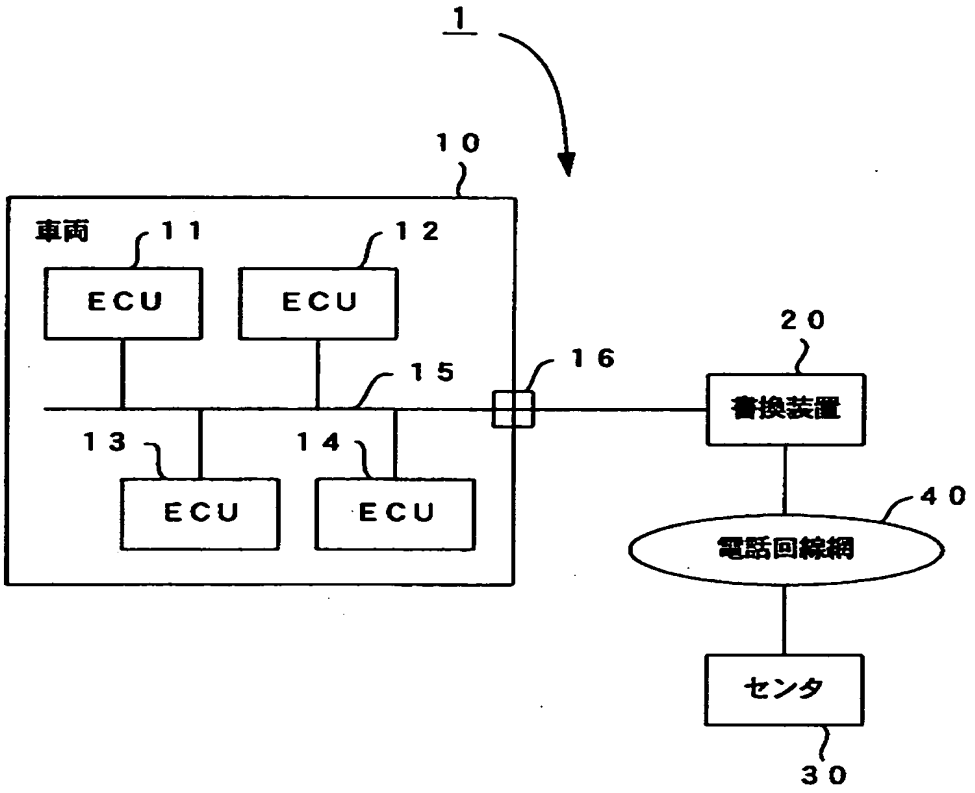
２０…書換装置

３０…センタ

４０…電話回線網

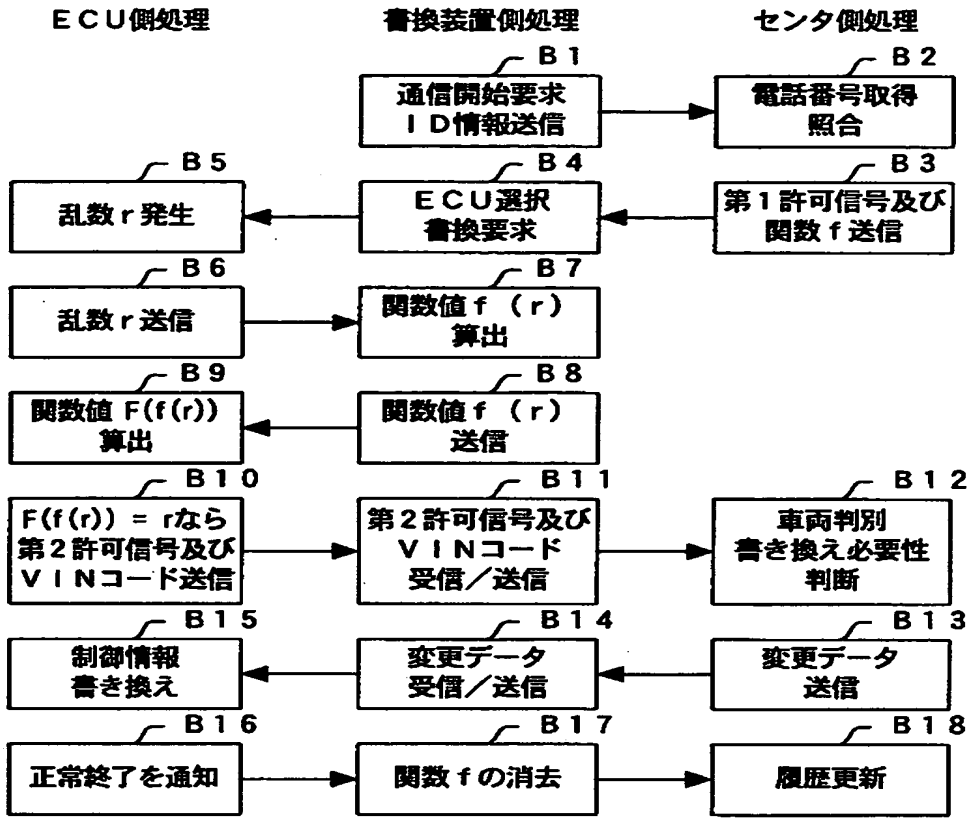
【書類名】　　図面

【図１】

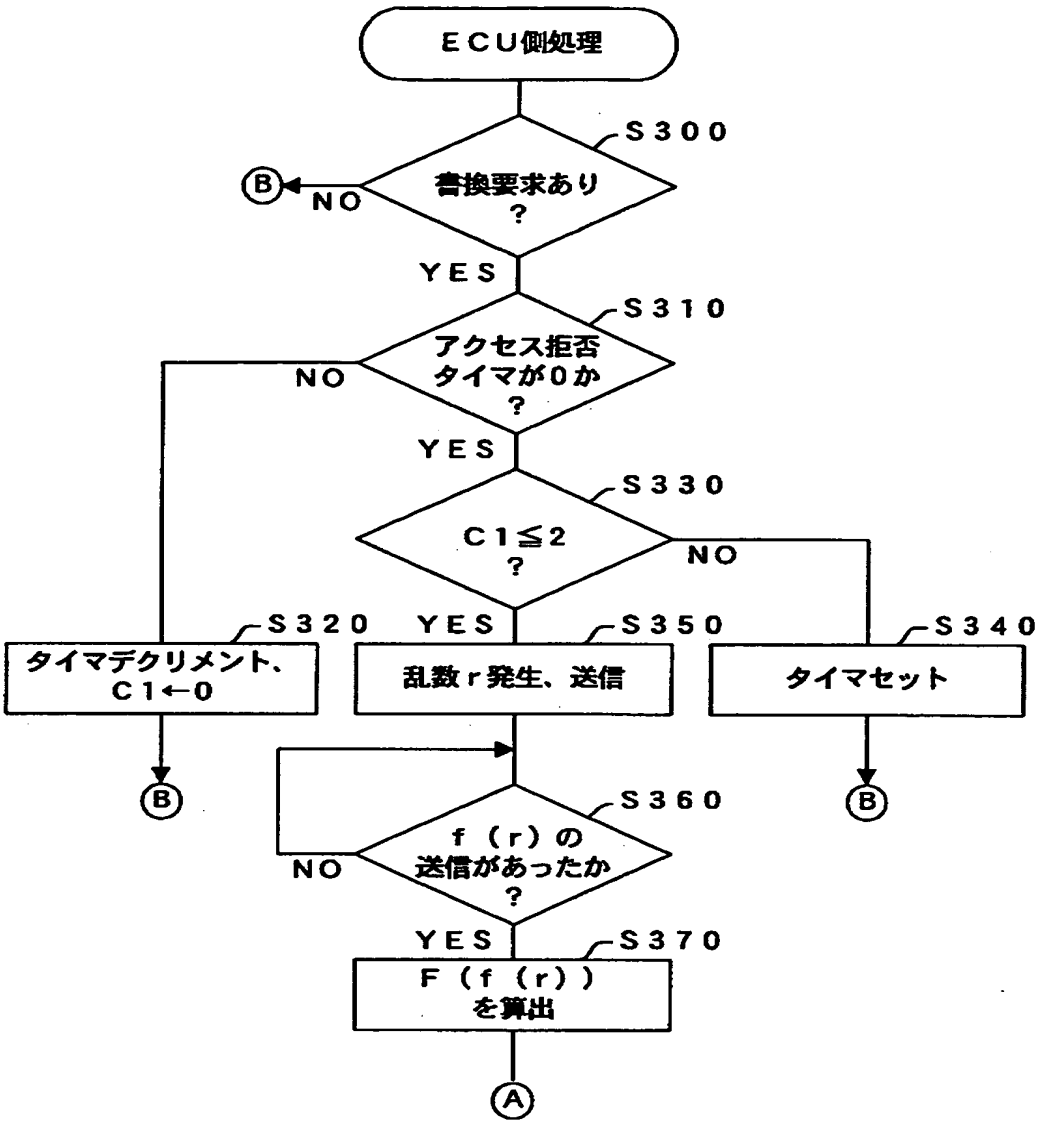


出証特２０００－３０９５８４１

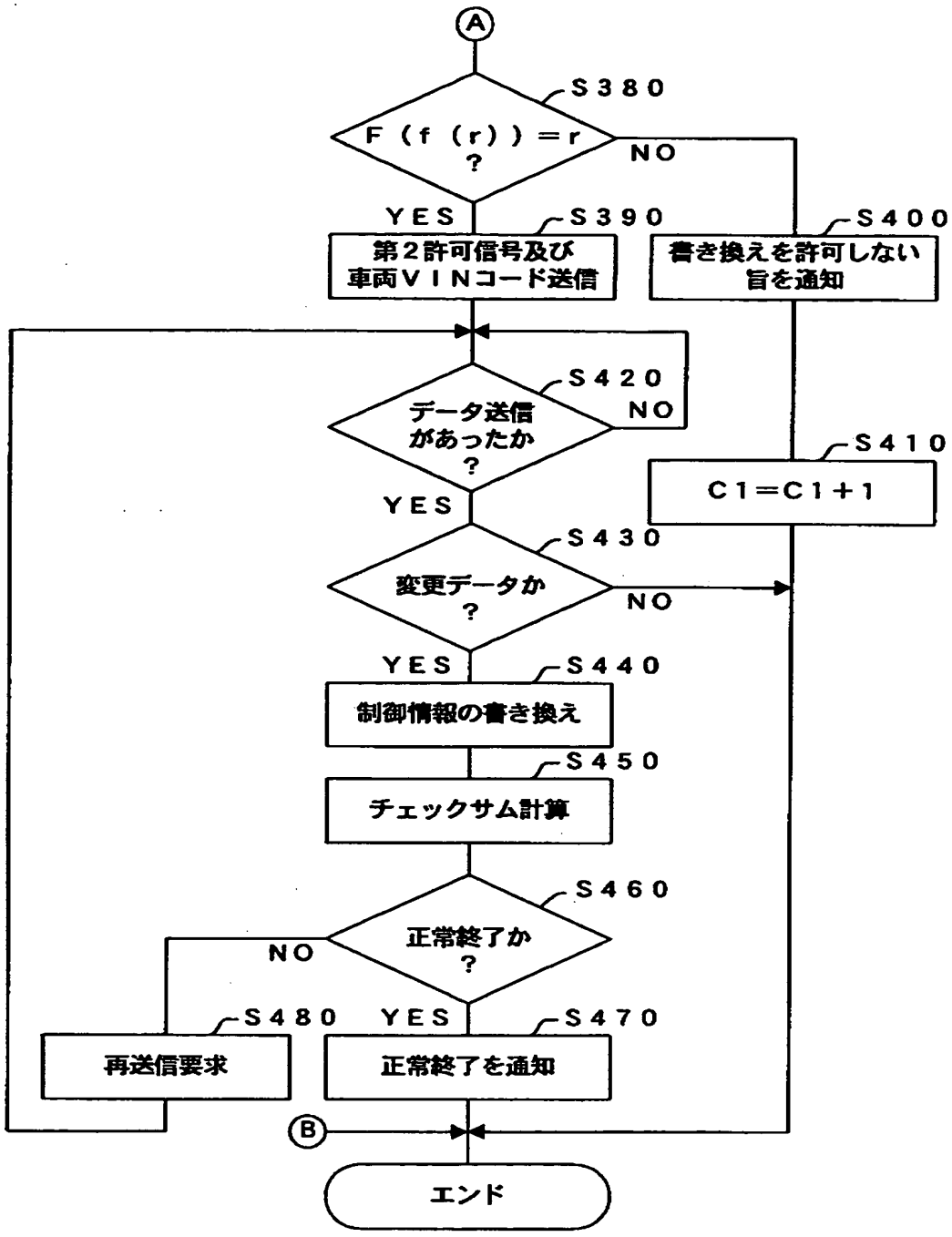
【図２】


ＥＣＵ側処理
書換装置側処理
センタ側処理
Ｂ１
通信開始要求
ＩＤ情報送信
Ｂ２
電話番号取得
照合
Ｂ５
乱数ｒ発生
Ｂ４
ＥＣＵ選択
書換要求
Ｂ３
第１許可信号及び
関数ｆ送信
Ｂ６
乱数ｒ送信
Ｂ７
関数値ｆ（ｒ）
算出
Ｂ９
関数値 F(f(r))
算出
Ｂ８
関数値ｆ（ｒ）
送信
Ｂ１０
F(f(r)) = rなら
第２許可信号及び
ＶＩＮコード送信
Ｂ１１
第２許可信号及び
ＶＩＮコード
受信／送信
Ｂ１２
車両判別
書き換え必要性
判断
Ｂ１５
制御情報
書き換え
Ｂ１４
変更データ
受信／送信
Ｂ１３
変更データ
送信
Ｂ１６
正常終了を通知
Ｂ１７
関数ｆの消去
Ｂ１８
履歴更新

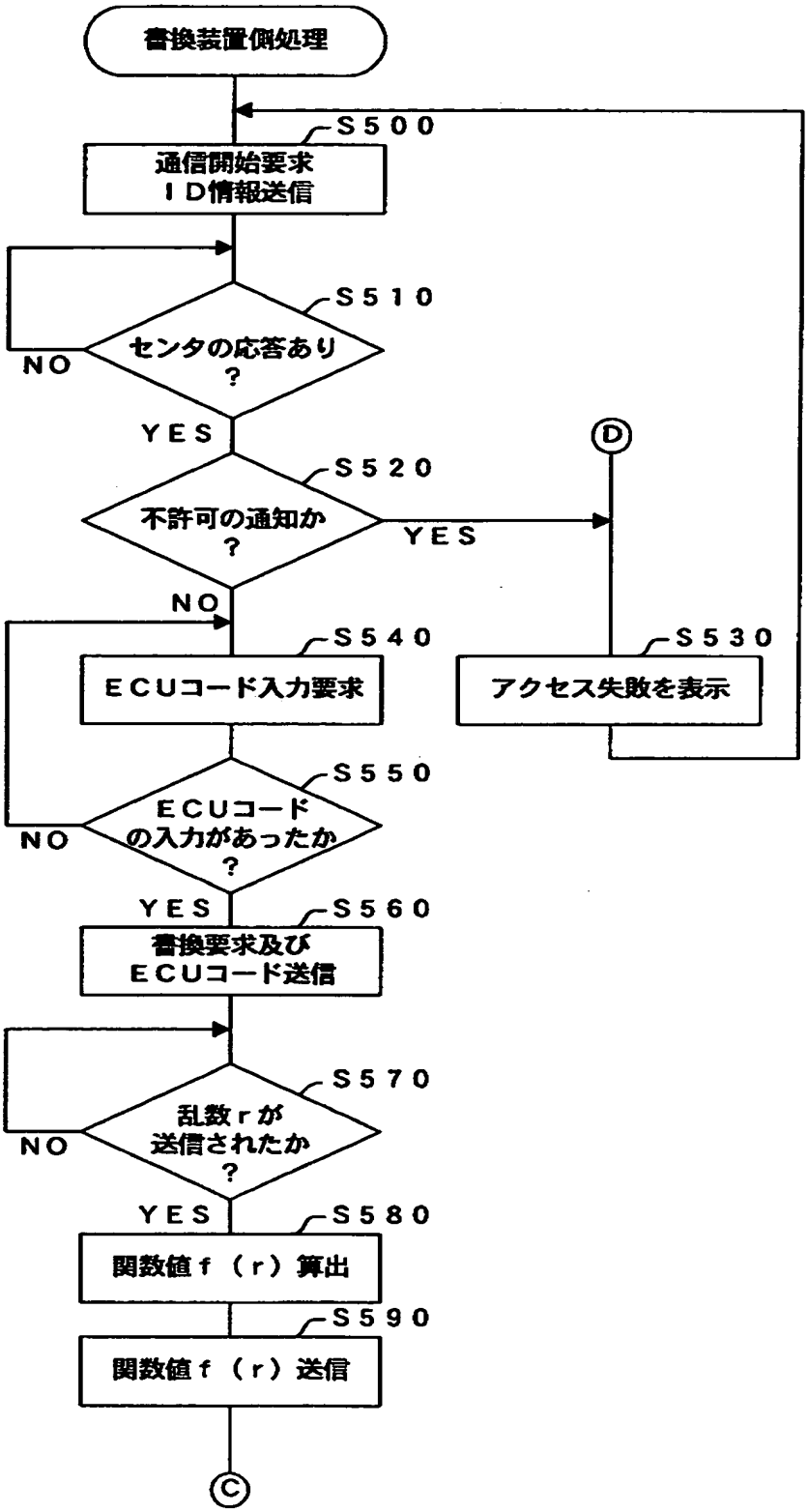
【図３】


ＥＣＵ側処理
Ｓ３００
書換要求あり
？
NO
Ⓑ
YES
Ｓ３１０
アクセス拒否
タイマが０か
？
NO
YES
Ｓ３３０
Ｃ１≦２
？
NO
YES
Ｓ３２０
タイマデクリメント、
Ｃ１←０
Ｓ３５０
乱数ｒ発生、送信
Ｓ３４０
タイマセット
Ⓑ
Ⓑ
Ｓ３６０
ｆ（ｒ）の
送信があったか
？
NO
YES
Ｓ３７０
Ｆ（ｆ（ｒ））
を算出
Ⓐ

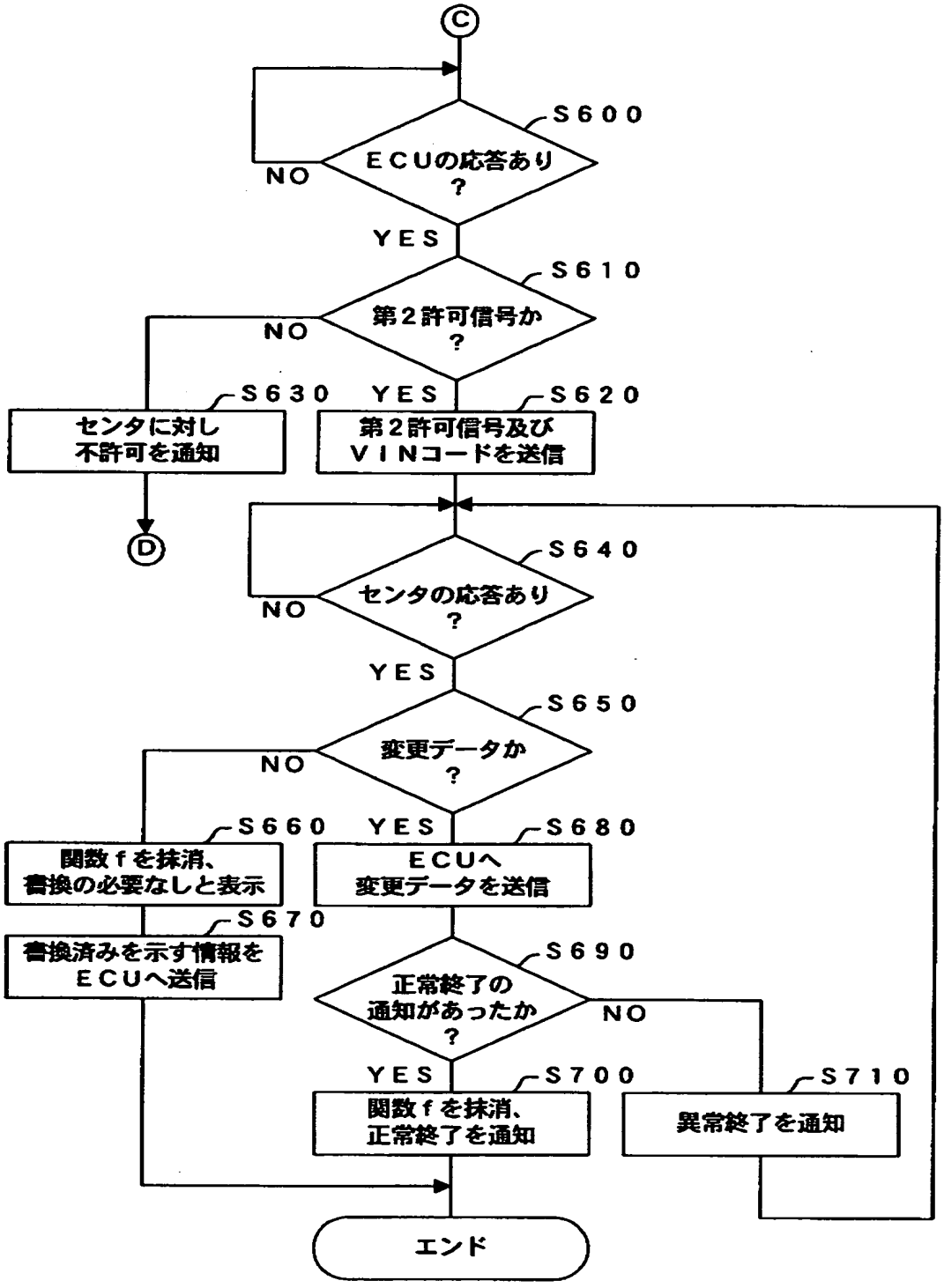
【図４】


A
S380
F（f（r））＝r
？
NO
YES
S390
第２許可信号及び
車両ＶＩＮコード送信
S400
書き換えを許可しない
旨を通知
S420
データ送信
があったか
？
NO
YES
S410
C1＝C1＋1
S430
変更データか
？
NO
YES
S440
制御情報の書き換え
S450
チェックサム計算
S460
正常終了か
？
NO
YES
S480
再送信要求
S470
正常終了を通知
B
エンド

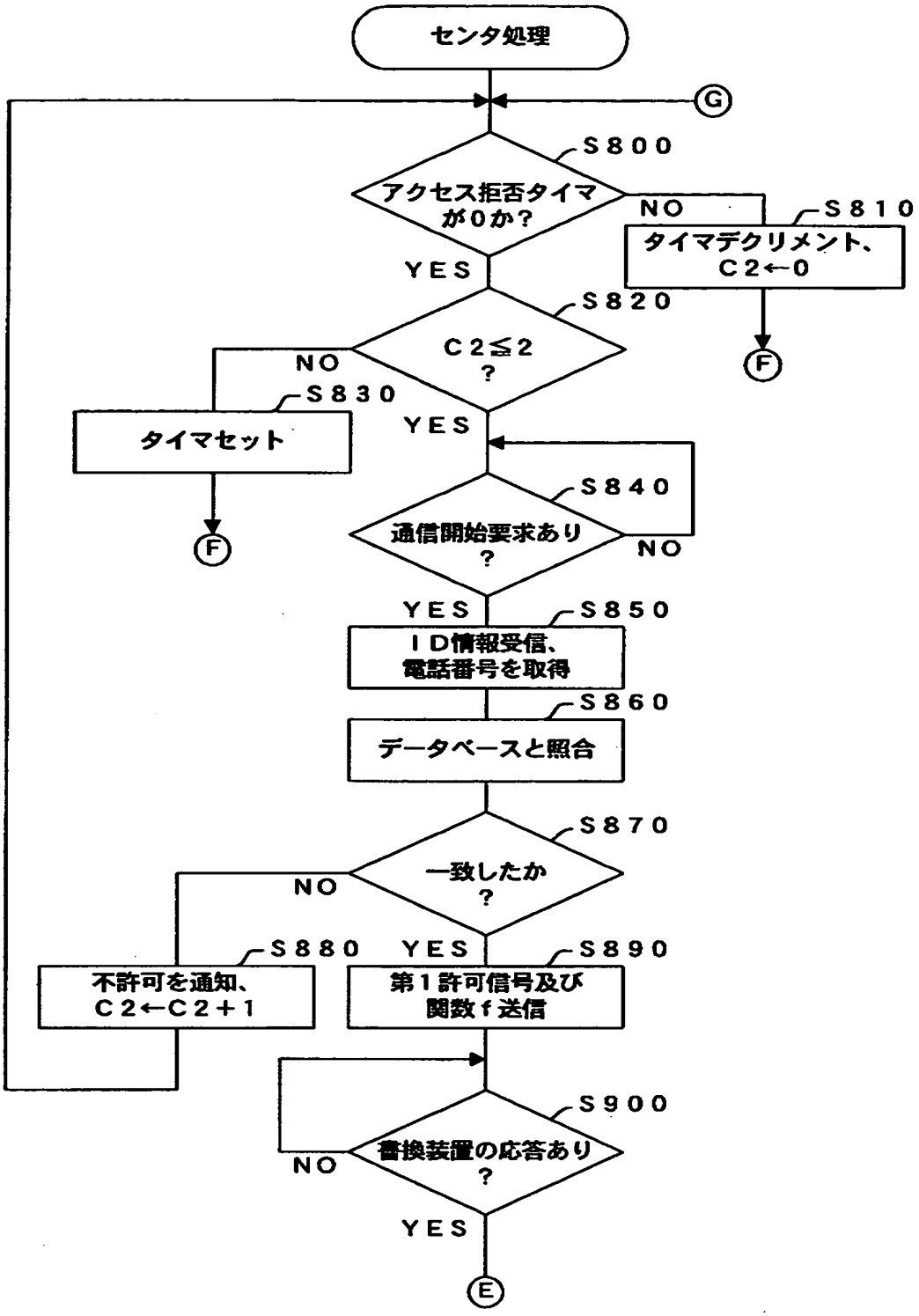
【図５】


書換装置側処理
S500
通信開始要求
ＩＤ情報送信
S510
センタの応答あり
？
NO
YES
S520
不許可の通知か
？
YES
D
NO
S540
ＥＣＵコード入力要求
S530
アクセス失敗を表示
S550
ＥＣＵコード
の入力があったか
？
NO
YES
S560
書換要求及び
ＥＣＵコード送信
S570
乱数ｒが
送信されたか
？
NO
YES
S580
関数値ｆ（ｒ）算出
S590
関数値ｆ（ｒ）送信
C

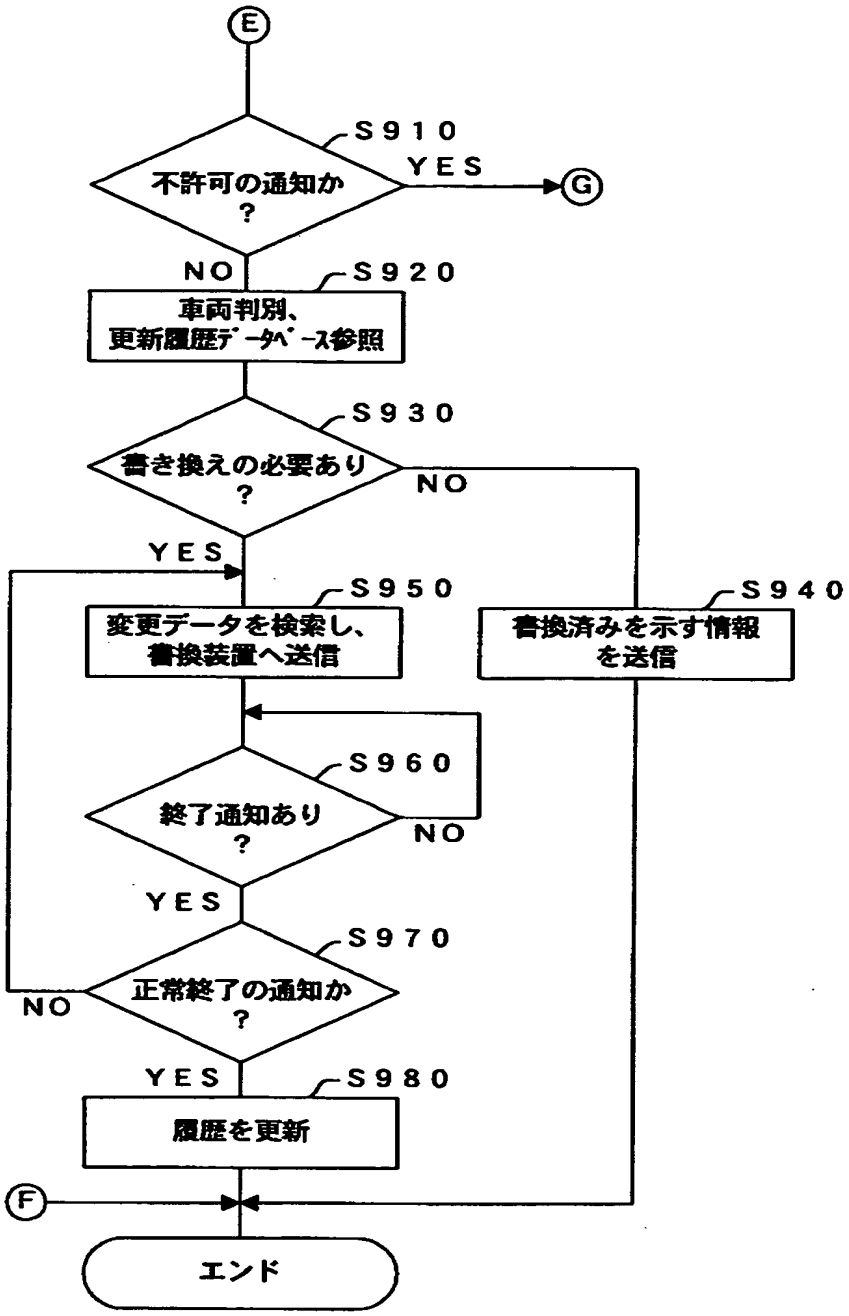
【図６】


Ⓒ
S600
ECUの応答あり？
NO
YES
S610
第2許可信号か？
NO
YES
S630
センタに対し不許可を通知
S620
第2許可信号及びVINコードを送信
Ⓓ
S640
センタの応答あり？
NO
YES
S650
変更データか？
NO
YES
S660
関数fを抹消、書換の必要なしと表示
S680
ECUへ変更データを送信
S670
書換済みを示す情報をECUへ送信
S690
正常終了の通知があったか？
NO
YES
S700
関数fを抹消、正常終了を通知
S710
異常終了を通知
エンド

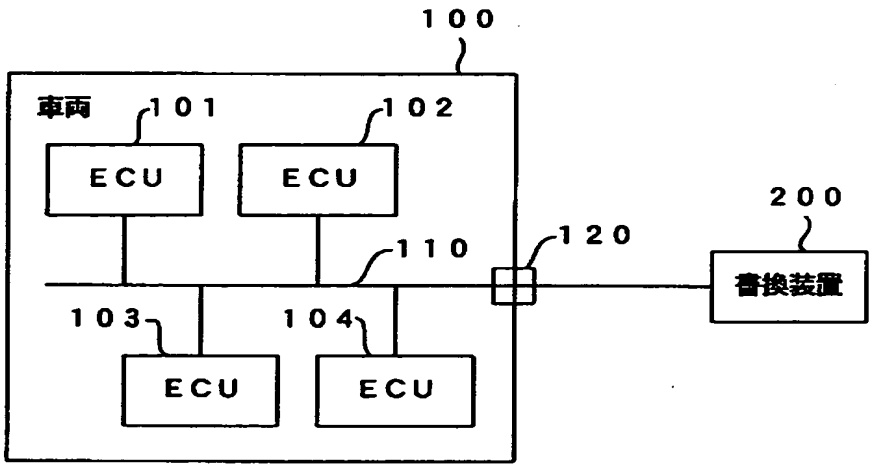
【図７】


センタ処理
G
S800
アクセス拒否タイマが0か？
NO
S810
タイマデクリメント、C2←0
YES
S820
C2≦2？
NO
S830
タイマセット
F
YES
S840
通信開始要求あり？
NO
YES
S850
ＩＤ情報受信、電話番号を取得
S860
データベースと照合
S870
一致したか？
NO
S880
不許可を通知、C2←C2＋1
YES
S890
第１許可信号及び関数ｆ送信
S900
書換装置の応答あり？
NO
YES
E

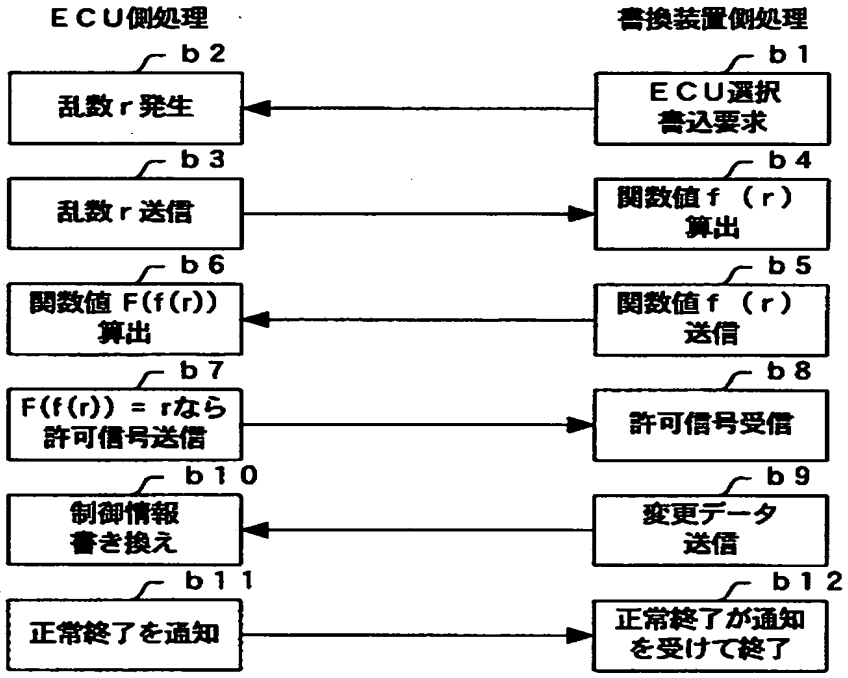
【図８】


E
S910
不許可の通知か？
YES
G
NO
S920
車両判別、更新履歴データベース参照
S930
書き換えの必要あり？
NO
YES
S950
変更データを検索し、書換装置へ送信
S940
書換済みを示す情報を送信
S960
終了通知あり？
NO
YES
S970
正常終了の通知か？
NO
YES
S980
履歴を更新
F
エンド

【図９】


１００
車両
１０１
１０２
ＥＣＵ
ＥＣＵ
２００
１１０
１２０
書換装置
１０３
１０４
ＥＣＵ
ＥＣＵ

【図１０】


ＥＣＵ側処理
書換装置側処理
ｂ２
乱数ｒ発生
ｂ１
ＥＣＵ選択
書込要求
ｂ３
乱数ｒ送信
ｂ４
関数値ｆ（ｒ）
算出
ｂ６
関数値 F(f(r))
算出
ｂ５
関数値ｆ（ｒ）
送信
ｂ７
F(f(r)) = rなら
許可信号送信
ｂ８
許可信号受信
ｂ１０
制御情報
書き換え
ｂ９
変更データ
送信
ｂ１１
正常終了を通知
ｂ１２
正常終了が通知
を受けて終了

【書類名】　　要約書

【要約】

【課題】　書換装置又は書換装置内部の情報が盗まれた場合であっても、電子制御装置における制御情報の不正な書き換えを防止できるようにする

【解決手段】　書換装置２０がＥＣＵ１１～１４にアクセスするために必要な関数ｆをセンタ３０に記憶しておく。そして、センタ３０は、書換装置２０を正当なものと判断してはじめて、書換装置２０へ関数ｆを送信する。センタ３０は、書換装置２０に対しユニークに割り振られたＩＤ情報と電話回線網４０を介してデータ通信を行う際の書換装置２０側の電話番号とを対応させて記憶したデータベースを有している。そして、書換装置２０からＩＤ情報を取得すると共に発呼元の電話番号を取得し、このＩＤと電話番号との対応関係がデータベースに記憶された対応関係と一致している場合に、書換装置２０を正当なものと判断する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２６０〕

１．変更年月日　　１９９６年１０月　８日
［変更理由］　名称変更
住　所　　愛知県刈谷市昭和町１丁目１番地
氏　名　　株式会社デンソー